



Docket GB920020044US2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Graeme G. Schreiber, et al;

Serial Number: 10/727,372

Filed: December 04, 2003

Title: Software Method For Improved Password Entry

Group Art Unit: 2121

Examiner: (unknown)

Customer 25299

TRANSMITTAL OF CERTIFIED COPY OF APPLICATION

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Dear Sir:

Enclosed please find the certified copy of the foreign application from which priority is claimed for the above-identified application:

Country: United Kingdom

Application Number: 0229727.3

Priority Date: December 19, 2002

Respectfully submitted,

Daniel E. McConnell

Registration No. 20,360

Telephone No.: (919) 543-1105

Fax No.: (919) 254-2649

Certificate of Mailing/Facsimile 37 CFR §1.8(a)

I hereby certify that this correspondence is being:

☒ deposited with the United States Postal Service as first class mail in an envelope with sufficient postage addressed to the:

☐ facsimile transmitted to fax #703-746-4060 to the:

Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 15, 2004

Michele Fitzsimmons

Person mailing/faxing document

Signature

THIS PAGE BLANK (USPTO)



INVESTOR IN PEOPLE

CERTIFIED COPY OF PRIORITY DOCUMENT

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

According to the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1985 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., L.C. or PLC.

Registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

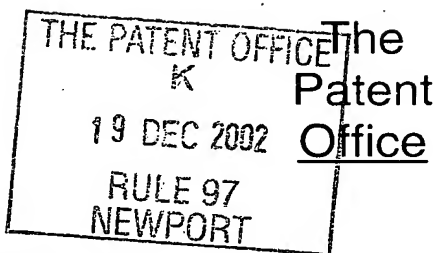
Dated 15 December 2003

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

1/77

Patents Act 1977
Rule 16



23DEC02 E772673-1 D00611
P01/7700 0.00-0229727.3

Request for grant of a patent

The Patent Office
Concept House
Cardiff Road
Newport
South Wales NP10 8QQ

1.	Your reference	GB920020044GB1		
2.	Patent application number (The Patent Office will fill in this part)	0229727.3		
3.	Full name, address and postcode of the or of each applicant (underline all surnames)	INTERNATIONAL BUSINESS MACHINES CORPORATION Armonk New York 10504 United States of America		
	Patents ADP number (if you know it)	519 637001		
	If the applicant is a corporate body, give the country/state of its incorporation	State of New York United States of America		
4.	Title of the invention	IMPROVED PASSWORD ENTRY		
5.	Name of your agent (if you have one)	C J Ling		
	"Address for Service" in the United Kingdom to which all correspondence should be sent (including the postcode)	IBM United Kingdom Limited Intellectual Property Department Hursley Park Winchester Hampshire SO21 2JN		
	Patents ADP number (if you know it)	70065001		
6.	If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number	Country	Priority App No (if you know it)	Date of filing (day/month/year)
7.	If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date or the earlier application	No of earlier application		Date of filing (day/month/year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.) Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description 8 ✓
Claim(s) 1 ✓
Abstract 1 ✓
Drawing(s) 10 + 10

10. If you are also filing any of the following, state how many against each item.

Priority documents
Translations of priority documents
Statement of inventorship and right to grant of a patent (Patents Form 7/77) 3
Request for preliminary examination and search (Patents Form 9/77)
Request for substantive examination (Patents Form 10/77)
Any other documents (please specify)

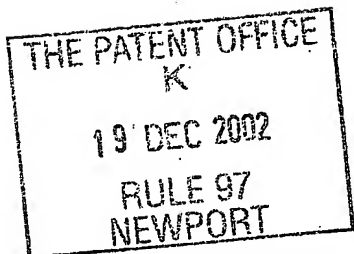
Handwritten mark

11. I/We request the grant of a patent on the basis of this application

C. J. Ling
Signature 17 December 2002
Date

12. Name and daytime telephone number of person to contact in the United Kingdom C J Ling
01962 815212

Patents Act 1977
Rule 15



The
Patent
Office

7/77

Statement of inventorship and of right to grant of a patent

The Patent Office
Concept House
Cardiff Road
Newport
South Wales NP10 8QQ

1. Your reference **GB920020044GB1**
2. Patent application number
(if you know it) **0229727.3**
3. Full name of the or of each applicant **INTERNATIONAL BUSINESS MACHINES CORPORATION**
4. Title of invention **IMPROVED PASSWORD ENTRY**
5. State how the applicant(s) derived the right
from the inventor(s) to be granted a patent **By virtue of employment and by agreement**
6. How many, if any, additional Patents Forms
7/77 are attached to this form?
7. I/We believe that the person(s) named over the page (and
on any extra copies of this form) is/are the inventor(s) of the
invention which the above patent application relates to.

C. J. Ling
Signature 17 December
2002
Date
8. Name and daytime telephone number of
person to contact in the United Kingdom **C J Ling**
Tel: 01962 815212

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

Graeme George **SCHREIBER**
Resident of UK
c/o IBM United Kingdom Limited
Intellectual Property Law
Hursley Park
Winchester
Hampshire SO21 2JN
England

Patents ADP number (if known)

Andrew Ramsay **KNOX**
Resident of UK
c/o IBM United Kingdom Limited
Intellectual Property Law
Hursley Park
Winchester
Hampshire SO21 2JN
England

Patents ADP number (if known)

If there are more than three inventors, please write their names and addresses on the back of another Patents Form 7/77 and attach it to this form

REMINDER

Have you signed the form?

Patents ADP number (if known)

IMPROVED PASSWORD ENTRY

Field of the Invention

5 The invention relates to the entry of passwords, codes or
identification numbers into data processing systems, Automated Teller
Machines, locks or other security or access control devices. More
particularly, the invention relates to the checking of the rhythm and tempo
10 used for entry of the password, code or identification number.

Background of the Invention

15 IBM Technical Disclosure Bulletin v.30, n.5, October 1987, p.258,
"Passwords for Computer Systems and Cipher Locks Containing Rhythm
Patterns" discloses the use of a password with timing constraints such as
the pauses between key-presses or the duration of the key-press being
added. The pauses or duration are predefined and may be either "long" or
short" and may be either relative to each other or absolute values.

20 US Patent 4,621,334 discloses a personal identification apparatus in
which a mean time between keystrokes is used to determine whether a person
attempting to gain access is the person who should be granted access to the
system.

25 US Patent 4,805,222 discloses a method of verifying a person's
identity by measuring the average inter-character time between successive
pairs of keystrokes and comparing this with a pre-stored sample.

30 US Patent 5,557,686 discloses a user verification system in which
vectors are constructed from user inputted samples and a neural network is
used to determine whether the user inputted samples are similar to a sample
entered for user verification.

35 US Patent 5,721,765 discloses a security system in which digits of an
identification number are separated into two or more groups that must be
entered with a predetermined time delay between each of the two or more
groups.

40 US Patent 6,151,593 discloses a neural network which compares a
timing vector extracted from the keystrokes a user has typed in with a
training set to authenticate the identity of the user.

It would be desirable to allow entry of a password, code or
identification number according to a rhythm and tempo defined by the user

entering the password, code or identification number during a learning period.

Disclosure of the Invention

Accordingly the invention provides a method of authenticating a user comprising the steps of: providing, by the user, a unique identifier, the unique identifier comprising both a sequence of keystrokes and the inter-keystroke intervals associated with provision of those keystrokes; comparing the unique identifier provided by the user with a reference unique identifier by: comparing the absolute inter-keystroke intervals of the unique identifier with the absolute inter-keystroke intervals of the reference unique identifier and returning a true indication if the absolute inter-keystroke interval of the unique identifier is within a predetermined tolerance of the absolute inter-keystroke interval of the reference identifier; comparing the relative inter-keystroke intervals of the unique identifier with the relative inter-keystroke intervals of the reference unique identifier and returning a true indication if the relative inter-keystroke interval of the unique identifier is within a predetermined tolerance of the relative inter-keystroke interval of the reference identifier; authenticating said user if both said absolute comparison step and said relative comparison step return a true indication.

The invention has the advantage that both the absolute inter-keystroke interval and the relative inter-keystroke interval are compared and if the two comparisons are sufficiently close, that is, within a predetermined tolerance, then the comparison is true. In this way a user can add a rhythm and a tempo to the way in which they enter the unique identifier.

Preferably, said relative inter-keystroke intervals are the ratio of the inter-keystroke intervals and the inter-keystroke interval between entry of the first of said sequence of keystrokes and the second of said sequence of keystrokes. The use of the relative inter-keystroke intervals being calculated as relative to the first inter-keystroke interval provides for simple computation of the required relative ratios.

In a preferred embodiment, the method further comprises the step of entry by the user of the reference unique identifier and wherein said predetermined tolerance is determined during said step of entry by the user of the reference unique identifier. This allows the method to determine the most appropriate tolerance from the initial entry of the reference unique identifier. The tolerance must be sufficiently large that authentication is not refused due to minor variations in entry of the

unique identifier, but also that authentication is not given when the unique identifier is not entered by the authorised user.

5 In a variation of the preferred embodiment, said predetermined tolerance is explicitly set by the user. In some applications, it may be determined that a particular tolerance should be used and that the user should achieve this tolerance in order for the unique identifier to be accepted. For example, if during entry of the reference unique identifier, there is a large variation in the relative or absolute values of the inter-keystroke intervals, then that would allow future entry of the unique identifier with a large tolerance. It may be desirable to limit the tolerance or to explicitly set the tolerance.

15 The invention also provides a computer program comprising computer program code means adapted to perform the steps of any one of the methods described above.

Brief Description of the Drawings

20 The invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a flow diagram of a learning mode of an embodiment of the present invention;

25 Figure 2 is a screen image at step 102 of figure 1;

Figure 3 is a screen image after step 104 of figure 1;

Figure 4 is a screen image after step 106 of figure 1;

Figure 5 is a screen image of the error indication displayed at step 110 of figure 1;

30 Figure 6 is a flow diagram of a secure mode of an embodiment of the present invention;

Figure 7 is a screen image of the error indication displayed at step 614 of figure 6;

35 Figure 8 is a screen image of the error indication displayed at step 610 of figure 6;

Figure 9 is a screen image of the error indication displayed at step 618 of figure 6; and

40 Figure 10 is a screen image of the tempo checking portion of the present invention.

Detailed Description of the Invention

When a password, code or identification number is entered into a system by a user, there is typically a rhythm associated with the entry of

the characters or numbers of the password, code or identification number. In the context of this patent application, rhythm is taken to mean absolute measures of the time interval between the entry of each character or number of the password and password is taken to mean a password, code or identification number. That is, for example, if the characters being entered are "fred", then the interval between entering "f" and "r" might be 203 ms, the interval between entering "r" and "e" might also be 203 ms and the interval between entering "e" and "d" might be 156 ms. Also, in the context of this patent application, Rhythm Tolerance is taken to mean the variation from these absolute values that are permitted for the rhythm of the entry of the password, code or identification number to be accepted. For example, using the intervals mentioned above, with a Rhythm Tolerance of 25%, a range of 153 ms to 253ms (203 ms plus or minus 25%) might be acceptable for the interval between entering "f" and "r" and a range of 117 ms to 195 ms (156 ms plus or minus 25%) might be acceptable for the interval between entering "e" and "d".

If the rhythm aspect of password entry is to be used, the system into which the password is entered must learn the rhythm associated with a password when it is first entered. The system does this by having a Learning Mode in which the password is entered and the rhythm is learnt. This might be a single entry of the password, but is preferably at least three entries of the password in order to allow for variation in entry of the password. Once the password has been learnt, a Secure Mode is used, in which the password is entered and checked.

Figure 1 shows a flow diagram of a Learning Mode of a first embodiment of the present invention. At step 102 (initialisation), a program window (shown in figure 2) is created on the screen. Referring to figure 2, the program window 200 has a window title 202 of "No Reference Password". A Rhythm Tolerance slider 204 is set to an initial value of 25%. Push-button 210 identifies that this is a Learn Mode. Push-button 206 to enter Secure Mode and tick-box 208 to Enable Rhythm Checking are initially disabled. The Enter Password window 212 is initially blank, ready for entry of a password. The message window 214 is initially empty.

At step 104 of figure 1, a first entry of a password is made. In the screen shot of the exemplary embodiment shown in figure 3, the window title 302 is now Reference Password: 'fred', since the password entered was "fred". A message is displayed in the message box 214 which says "New reference password accepted. The password that was typed in appears in the Enter Password window 212 and learn count window 218 has the text "0 Learnt" displayed in it because although one password entry has been made, this has been used to determine what characters or numbers the password

consists of. In alternative embodiments, this first entry of the password could be used as part of the learning process.

At step 106 of figure 1, a second entry of the password is made. Figure 4 shows a screen shot taken after the second entry of the password has been made. As each character of the password is entered, it is displayed in the message box 214 with the elapsed time interval between entry of each character in ms shown. Additionally, an acceptable range of time intervals computed using the rhythm tolerance may be shown. In the example of figure 4, this is not shown until a third entry of the password had been made, although this is not an essential feature of the invention and it could be shown after a first entry, or a second entry or a subsequent entry of the password.

When the Enter key or another key representing completion of the password entry process is pressed, then processing moves to step 108 of figure 1. If the second entry of the password matched the first entry of the password, the words "Password accepted." are displayed and the learn count window 218 now displays a learn count of 1. Processing moves to step 112 of figure 1 where an acceptable range of rhythm values is set. As an example, the message window of a subsequent entry might show:

```
'f' (0 ms) [Range: 0 -> 0] PASS
'r' (265 ms) [153 -> 253] FAIL (Slow)
'e' (203 ms) [153 -> 253] PASS
'd' (157 ms) [117 -> 195] PASS
Password accepted.
```

In the example above, the acceptable rhythm range has been set between 153 ms and 253 ms for the time interval between entry of "f" and "r", that is the time interval for the initial entry with a 25% tolerance applied. Similarly, for the time interval between entry of "r" and "e" and for "e" and "d", where the ranges are 153 ms to 253 ms and 117 to 195 ms respectively. The time interval between entry of "f" and "r" was outside the acceptable range and so failed for that entry. The time intervals between entry of "r" and "e" and for "e" and "d" were within the acceptable ranges for those time intervals and so passed for those entries.

If the second entry of the password does not match the first entry of the password, processing passes to step 110 of figure 1. Figure 5 shows a screen shot taken after an incorrect second entry of the password has been made. The words "Password text incorrect." and "Password not accepted." are displayed in the message window 214 and the learn count displayed in

the learn count window 218 is not incremented. An "Invalid Entry" indication 502 is displayed in the program window 500.

Once sufficient entries of the correct password have been made for a valid acceptable rhythm range to be determined, then at step 114 of figure 1, a Secure Mode is enabled and the push-button 206 for the Secure Mode may be selected. At step 116 of figure 1, a check is made as to whether the Secure Mode has been selected. If the Secure Mode has been selected, then the Learning Mode is exited at step 118 of figure 1 and the Secure Mode (described later with reference to figure 6) is entered.

If the Secure Mode is not selected, then subsequent entries of the password can be made at step 120 of figure 1. At step 122 of figure 1 a test is done to see if a subsequent entry matches the first entry. If a subsequent entry does match a first entry, then at step 124 of figure 1 the acceptable range is modified to take into account the values of the subsequent entry and processing returns to step 116 of figure 1. If a subsequent entry does not match the first entry, then an error indication is displayed at step 126 before processing returns to step 116 of figure 1.

Referring now to figure 6 which shows a flow diagram of a Secure Mode. A secure mode is entered at step 602. Rhythm checking is allowed, although not enabled at step 604. This is achieved in the exemplary embodiment by allowing selection of the tick box (208 in figure 7) but not having the tick box ticked by default. At step 606, the password is entered by the user.

At step 608, a check is made as to whether or not the password text is correct. If the password text is not correct, then "Password text incorrect" and "Password not accepted" messages are displayed in the message box (214 in figure 8) and an indication (502 in figure 8) is provided that the password is an invalid entry and an indication (802 in figure 8) is provided that the password is not accepted. Processing returns to step 606 to accept the entry of password. If the password text is correct, then at step 612, a check is made as to whether rhythm checking is enabled. If rhythm checking is not enabled, then at step 614 the password is accepted and a "Password accepted" message is displayed in the message box (214 in figure 7) and an indication (702 in figure 7) is displayed that the password is accepted.

If rhythm checking is enabled, then at step 616, the individual time intervals are checked to see if they fall within the respective ranges for those time intervals. If any of the time intervals do not fall within the acceptable ranges, then "Password rhythm incorrect" and "Password not

accepted" messages are displayed in the message box (214 in figure 9) and an indication (802 in figure 9) is provided that the password is not accepted. Processing returns to step 606 to accept the entry of password. If all of the time intervals fall within the acceptable ranges, then at
5 step 620 the password is accepted and a "Password accepted" message is displayed in the message box (214 in figure 7) and an indication (702 in figure 7) is displayed that the password is accepted.

In addition to checking the rhythm of entry of the password, the tempo is checked. In the context of this patent application, tempo is taken to mean relative measures of the time interval between the entry of each character or number of a password, code or identification number. That is, for example, if the characters being entered are "fred", then the interval between entering "f" and "r" might be 203 mS, the interval between
15 entering "r" and "e" might also be 203 mS and the interval between entering "e" and "d" might be 156 mS. The first inter-character interval, that is, the interval between entering "f" and "r", may be used as an "anchor" for checking the relative timing for the rest of the password. The second and subsequent inter-character intervals are divided by this first interval to give values for the tempo. So the Tempo value for the interval between
20 entering "r" and "e" would be 203 mS divided by 203 mS, that is 1.00 and the Tempo value for the interval between entering "e" and "d" might be 156 mS divided by 203 mS, that is 0.77. In an alternative embodiment, the average of the inter-character intervals may be used as an "anchor".

Also, in the context of this patent application, Tempo Tolerance is taken to mean the variation from these Tempo (relative) values that are permitted for the rhythm of the entry of the password, code or identification number to be accepted. For example, using the intervals
30 mentioned above, with a Tempo Tolerance of 25%, a Tempo value of 0.75 to 1.25 (1.00 plus or minus 25%) might be acceptable for the interval between entering "r" and "e" and a range of 0.58 to 0.96 (0.77 plus or minus 25%) might be acceptable for the interval between entering "e" and "d".

As for the rhythm aspect of password entry, the system into which the password is entered must learn the tempo associated with a password when it is first entered. The system does this by using a Learning Mode and a Secure Mode in which the password is entered and the tempo is learnt.

Figure 10 shows a program window 1000 with a window title 202 of "Reference Password: "fred". A Rhythm Tolerance slider 204 is set to an initial value of 25% and a Tempo Tolerance slider 1002 is set to an initial value of 25%. Tick-box 1004 is included to enable Tempo checking. Message window 214 shows the elapsed time interval between entry of each character

in ms, the range that is acceptable and whether the time interval is within the acceptable range. Additionally or alternatively for this embodiment, the reference tempo is shown, together with the minimum and maximum values and whether or not the tempo is within the tolerance range.

5 Additionally, the embodiment of figure 10 includes a graphical display 1006 of the rhythm and a graphical display 1008 of the tempo. The nominal value is shown together with the acceptable range. Additionally, the actual value for this entry is shown. It can then be seen graphically
10 whether or not the actual value falls within the accepted range.

15 Figures 2 to 5 and 7 to 10 and the associated description describe an embodiment that is a demonstration of the principles of the present invention. Considerable feedback is provided to the user in the embodiments described in order for the user to understand how the invention works and in order to allow the reader of this specification to fully understand the invention. Practical implementations of the invention which fall within the claims are likely not to include all of these features. For example, it is unlikely that the window title of a practical
20 implementation would include the test of the password itself. This password text has been included for the assistance of readers of this specification only. The embodiments described might be implemented in a manner similar to that described for the learning mode, but for the secure mode a minimal user interface is likely to be used with the user merely
25 being asked to provide a password and being informed whether or not that password has been accepted, without being told why it was not accepted. However, the principles of figures 1 and 6 are likely to be implemented.

30 Whilst the preferred embodiments of the present invention have been described here in detail, it will be clear to those skilled in the art that many variants are possible without departing from the spirit and scope of the present invention.

CLAIMS

1. A method of authenticating a user comprising the steps of:

5 providing, by the user, a unique identifier, the unique identifier comprising both a sequence of keystrokes and the inter-keystroke intervals associated with provision of those keystrokes;

comparing the unique identifier provided by the user with a reference unique identifier by:

10 comparing the absolute inter-keystroke intervals of the unique identifier with the absolute inter-keystroke intervals of the reference unique identifier and returning a true indication if the absolute inter-keystroke interval of the unique identifier is within a predetermined tolerance of the absolute inter-keystroke interval of the reference identifier;

15 comparing the relative inter-keystroke intervals of the unique identifier with the relative inter-keystroke intervals of the reference unique identifier and returning a true indication if the relative inter-keystroke interval of the unique identifier is within a predetermined tolerance of the relative inter-keystroke interval of the reference identifier;

20 authenticating said user if both said absolute comparison step and said relative comparison step return a true indication.

25 2. A method as claimed in claim 1, wherein said relative inter-keystroke intervals are the ratio of the inter-keystroke intervals and the inter-keystroke interval between entry of the first of said sequence of keystrokes and the second of said sequence of keystrokes.

30 3. A method as claimed in claim 1, further comprising the step of entry by the user of the reference unique identifier and wherein said predetermined tolerance is determined during said step of entry by the user of the reference unique identifier.

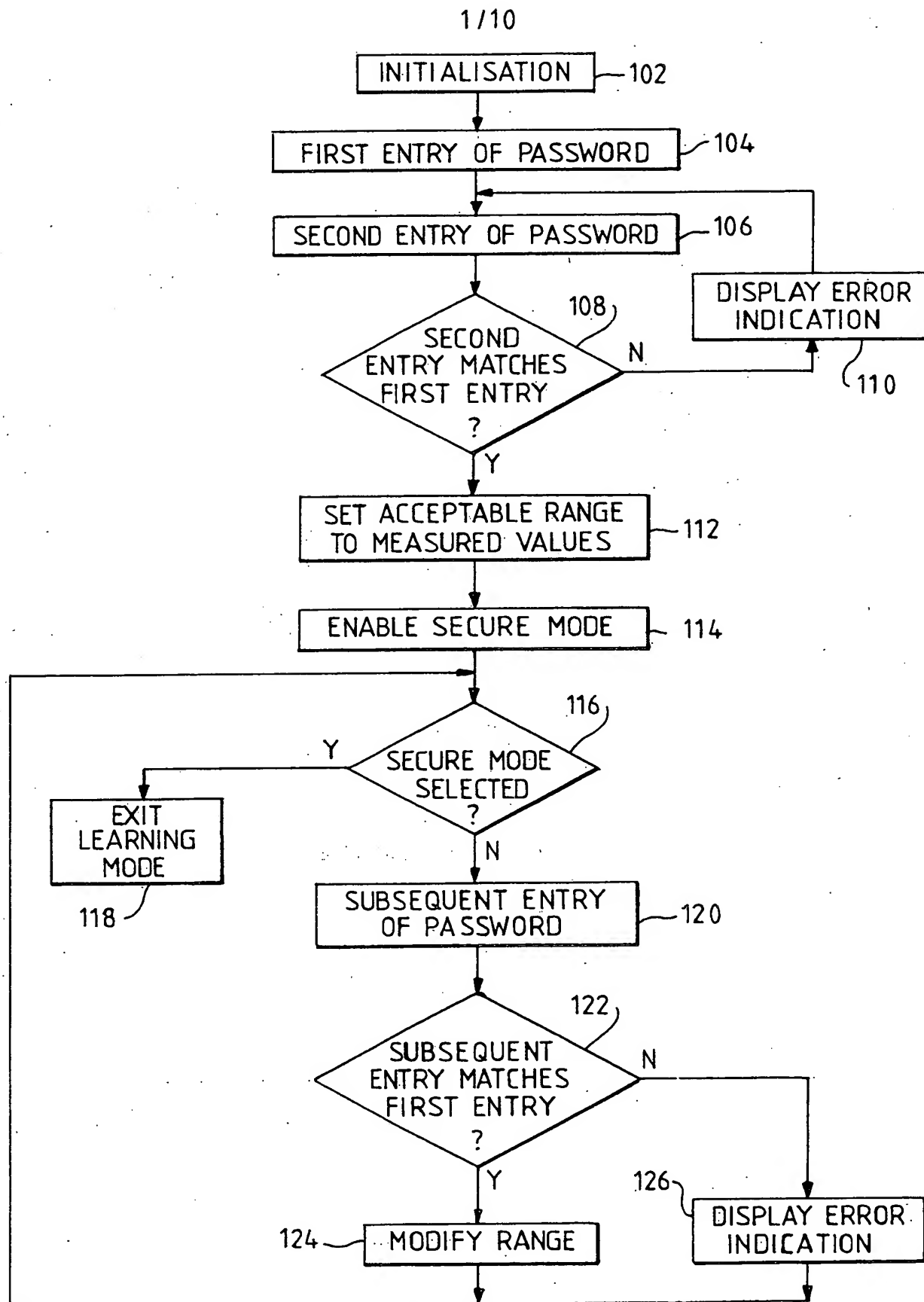
35 4. A method as claimed in claim 3 wherein said predetermined tolerance is explicitly set by the user.

5. A computer program comprising computer program code means adapted to perform the steps of any one of claim 1 to claim 4.

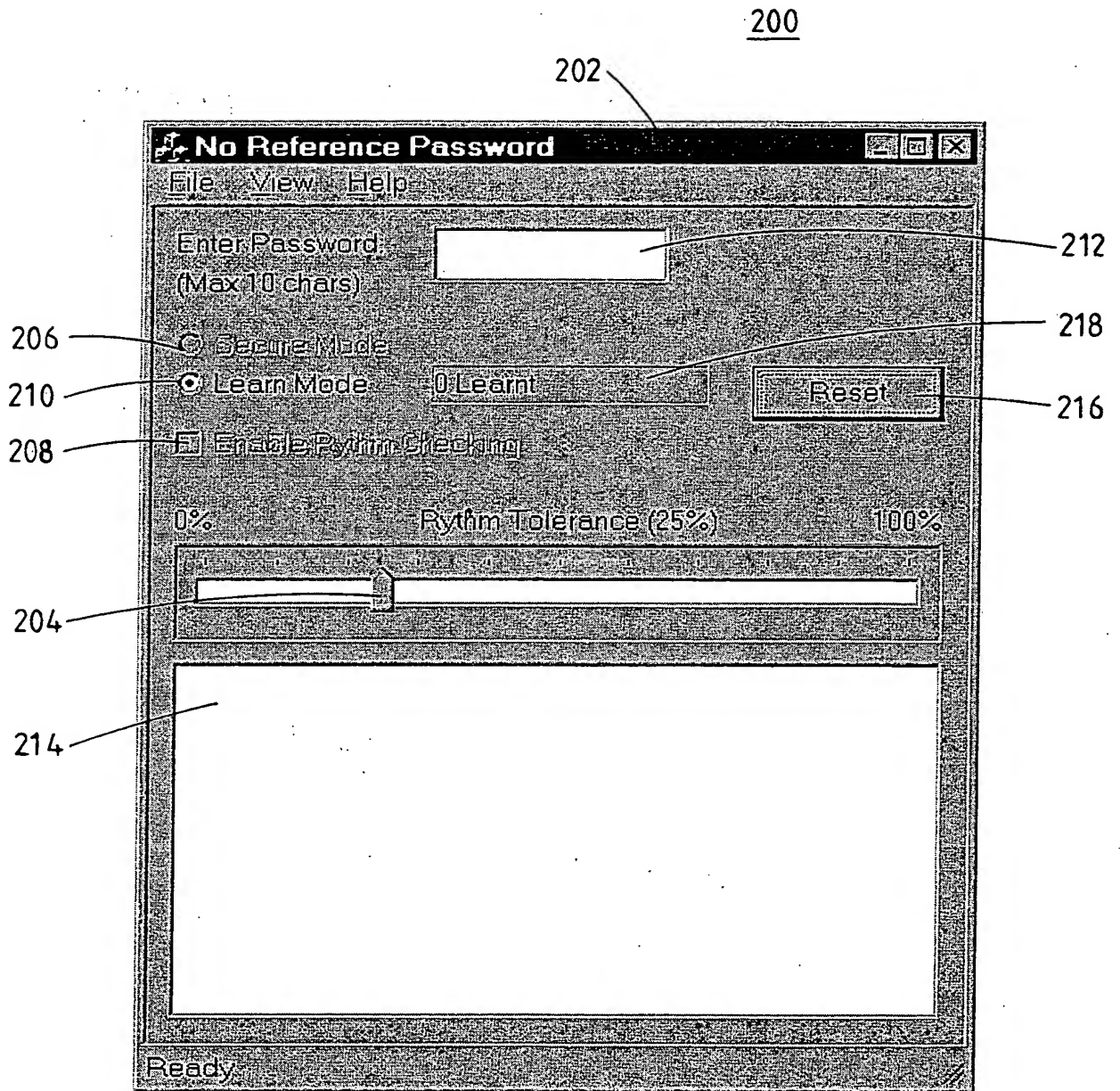
IMPROVED PASSWORD ENTRY

ABSTRACT

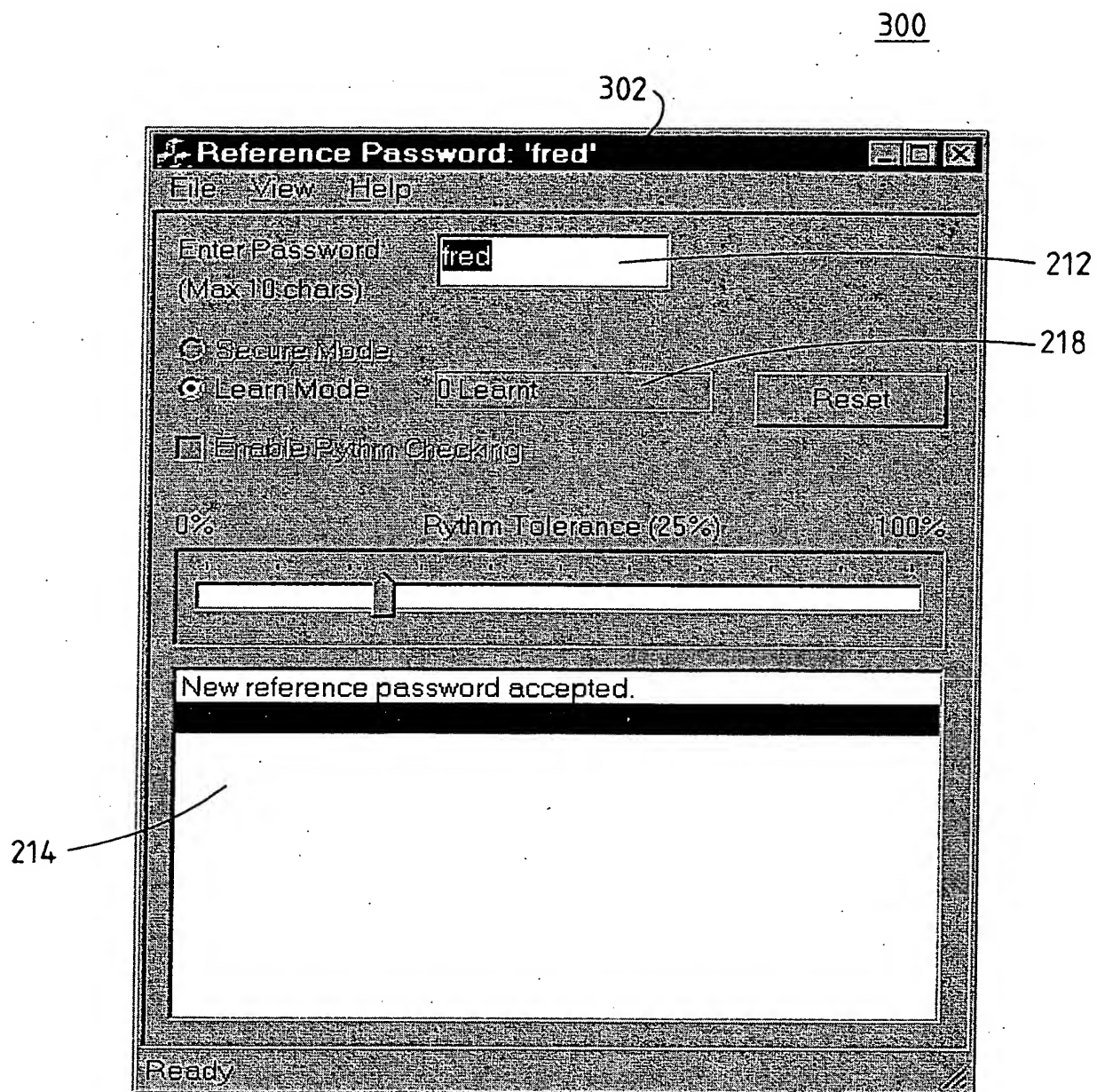
5 A method of authentication is described that uses both relative and
absolute values of inter-keystroke intervals measured during entry of a
unique identifier. Both the relative and absolute values have to be
achieved during entry of the unique identifier. The relative values are
the ratio of each of the inter-keystroke intervals divided by one of the
.0 inter-keystroke intervals or divided by the average inter-keystroke
interval.

**FIG.1**

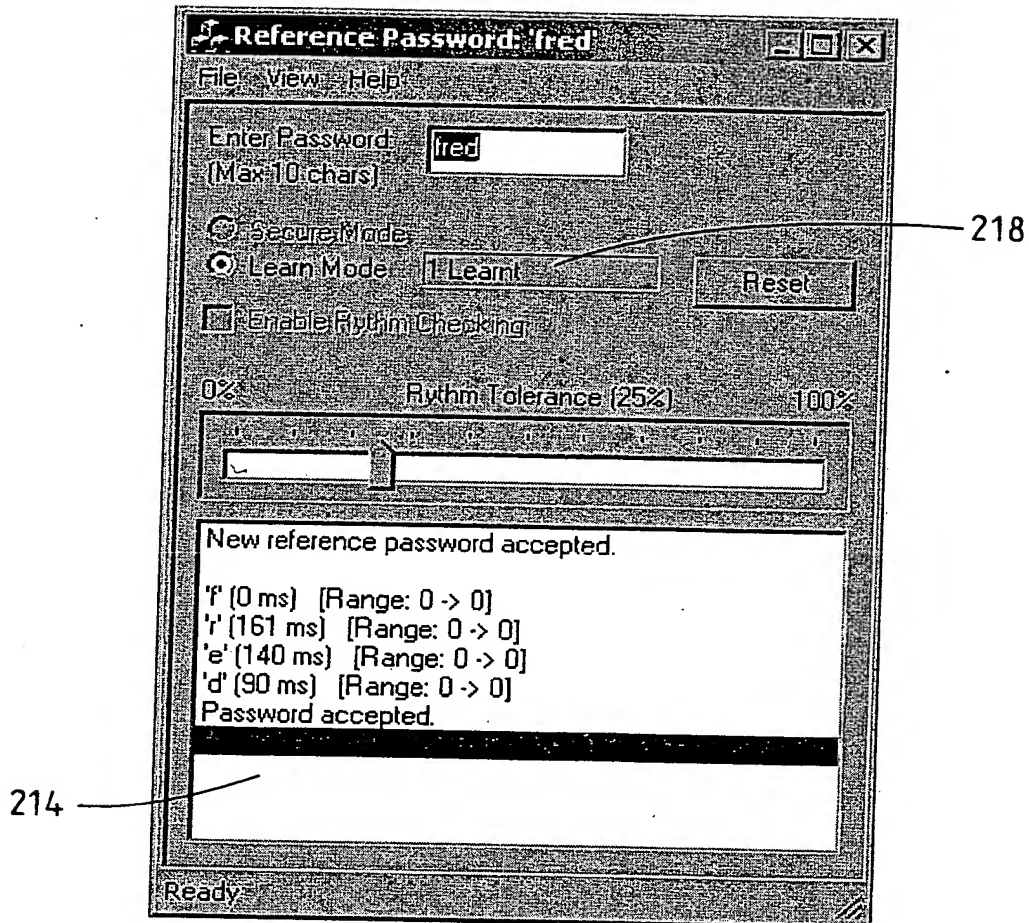
THIS PAGE BLANK (USPTO)

FIG. 2

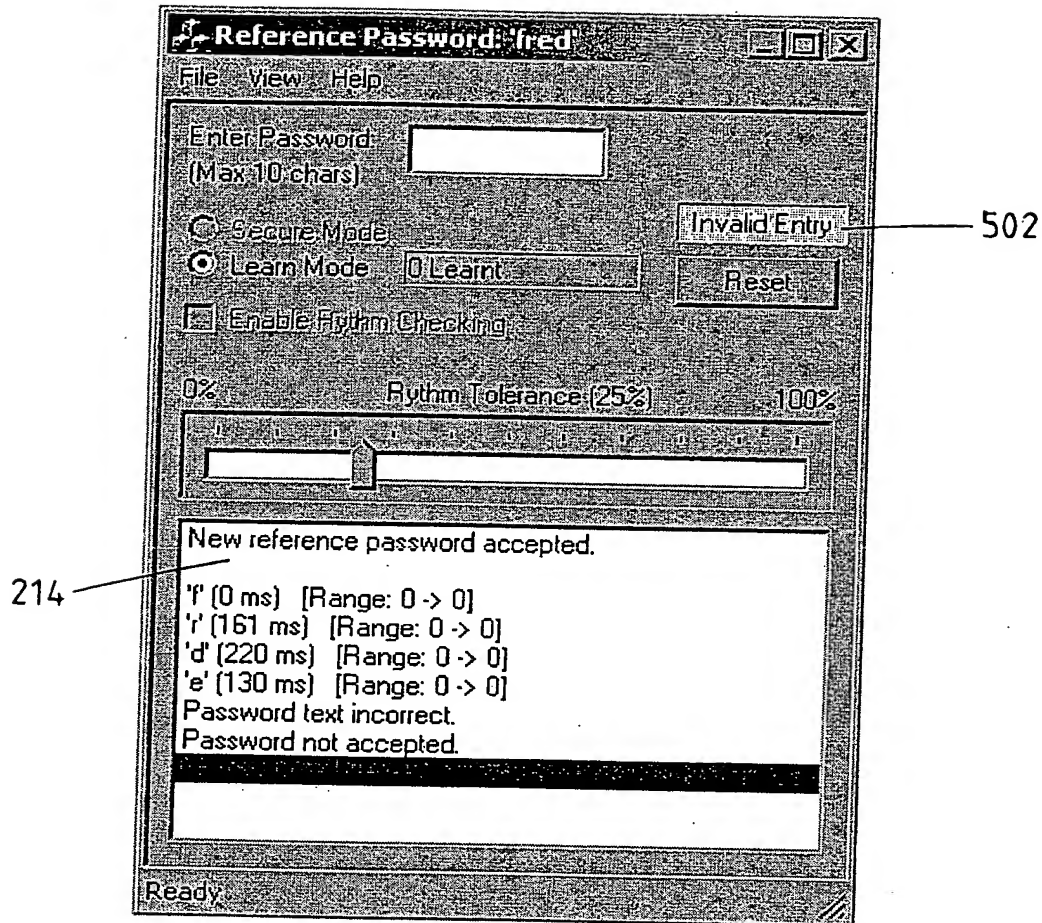
THIS PAGE BLANK (USPTO)

FIG. 3

THIS PAGE BLANK (USPTO)

FIG. 4

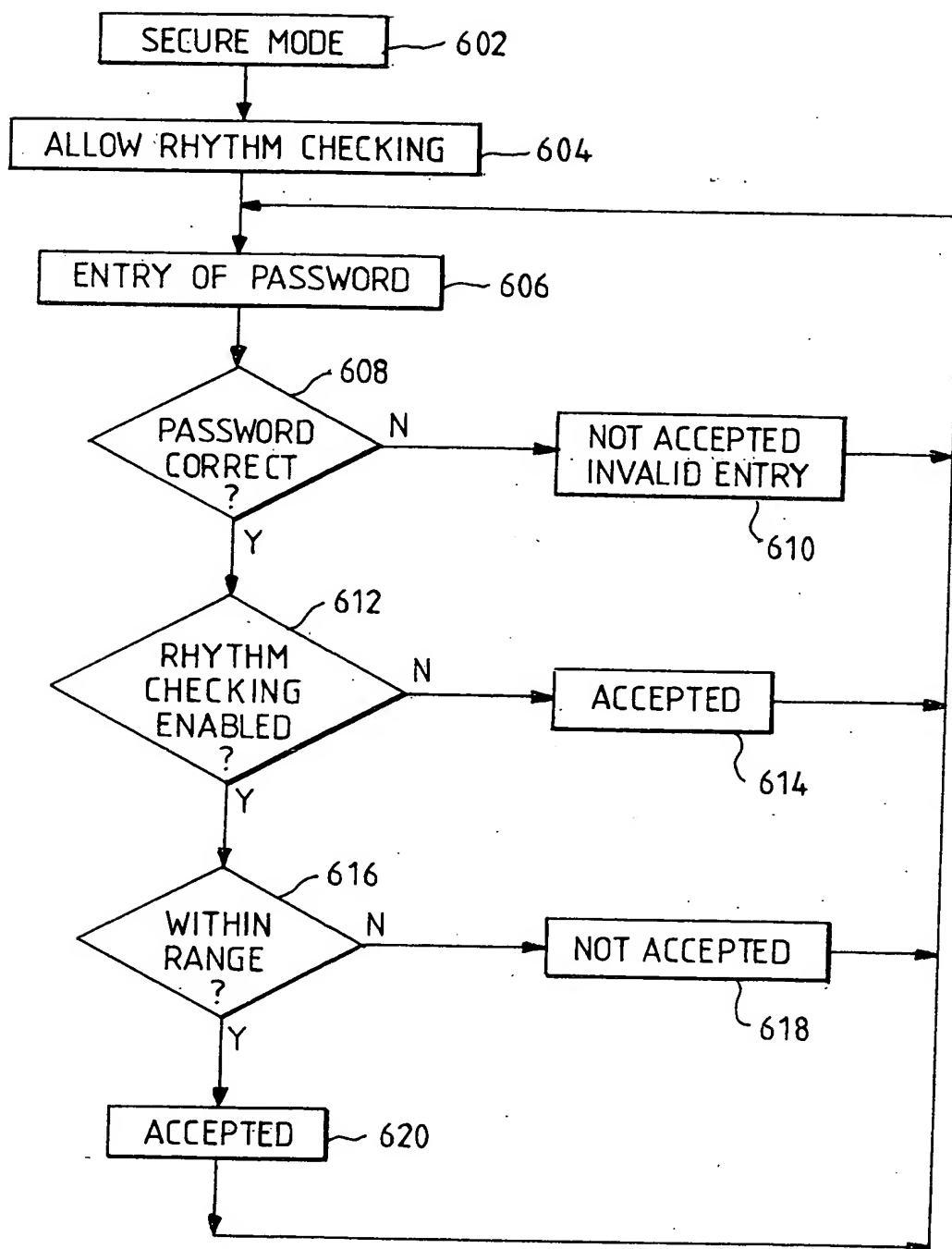
THIS PAGE BLANK (USPTO)

500FIG. 5

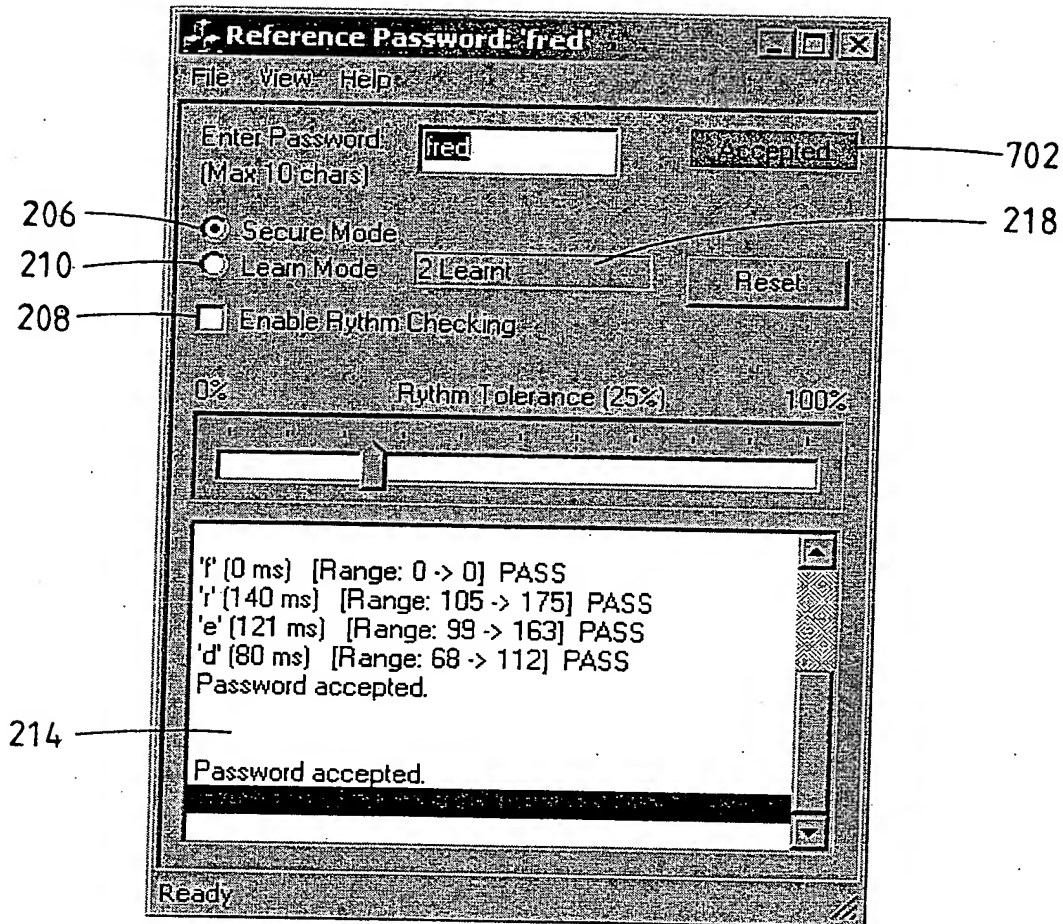
BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

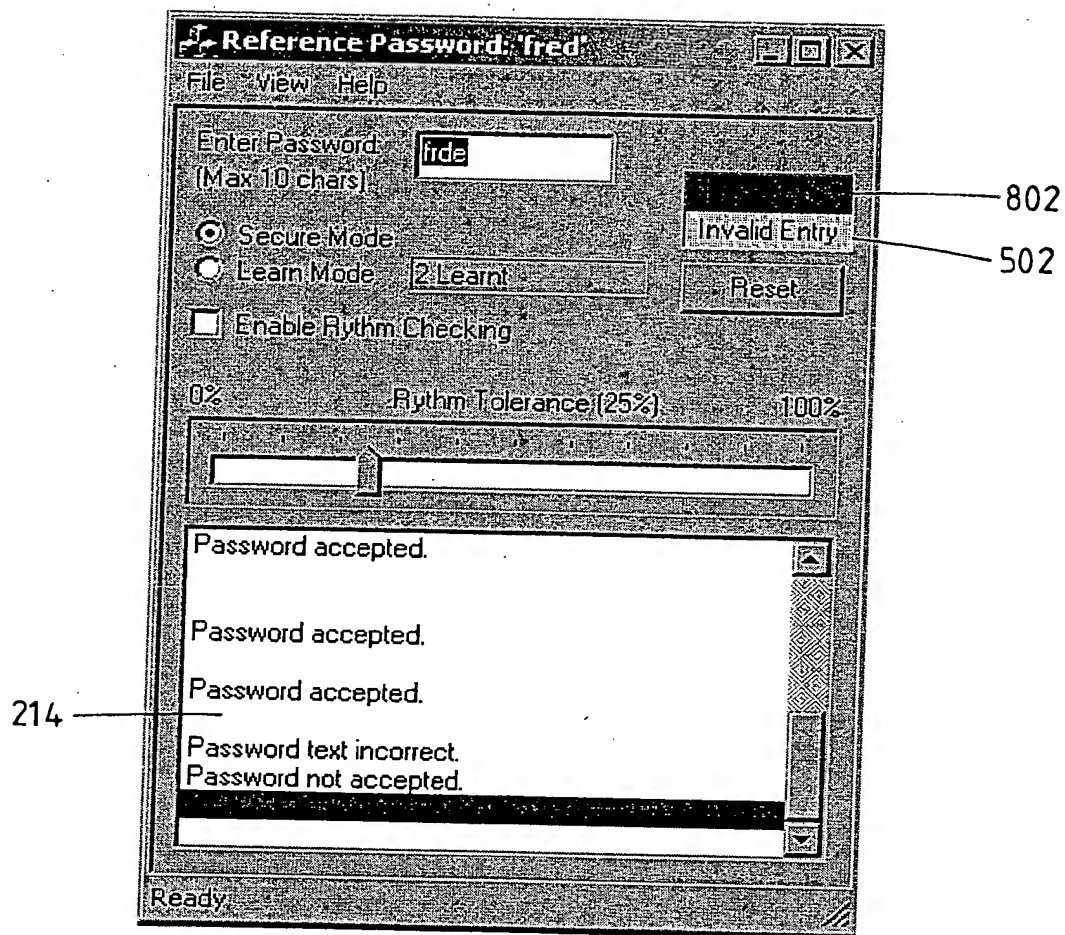
6/10

FIG. 6

THIS PAGE BLANK (USPTO)

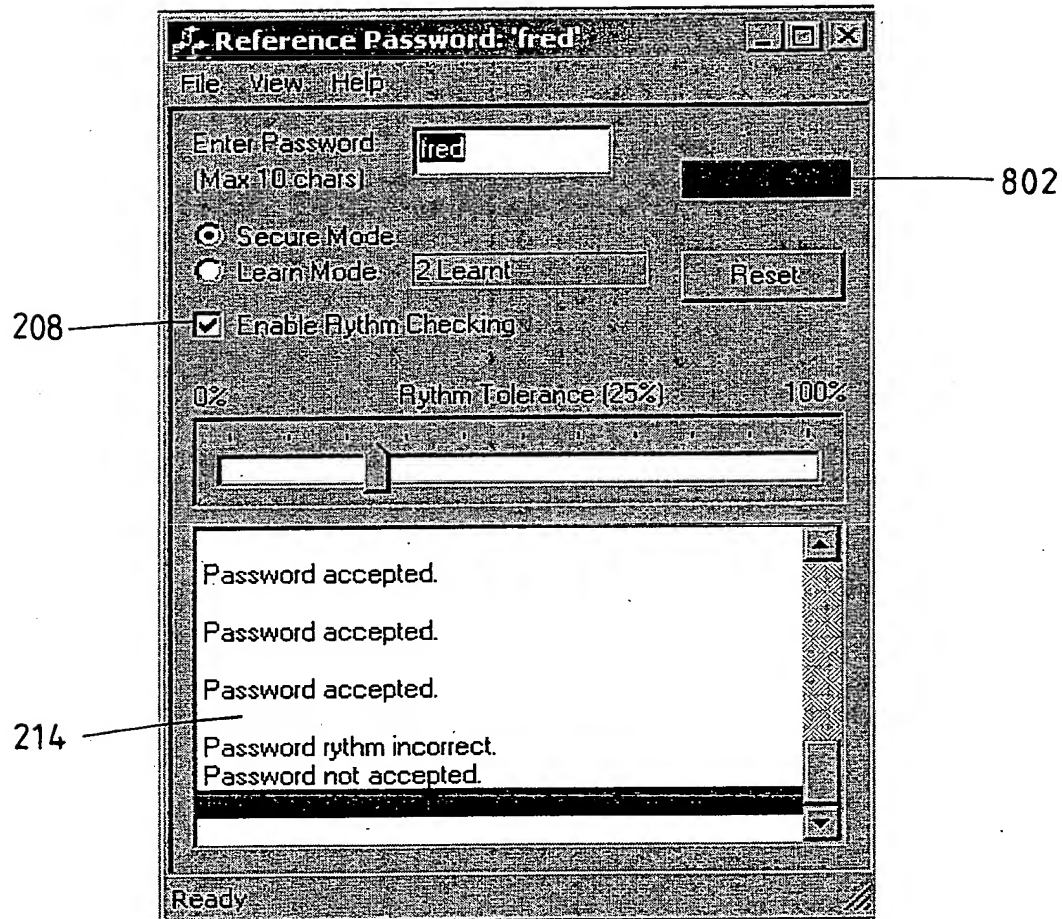
FIG. 7

THIS PAGE BLANK (USPTO)

800FIG. 8

THIS PAGE BLANK (USPTO)

9/10

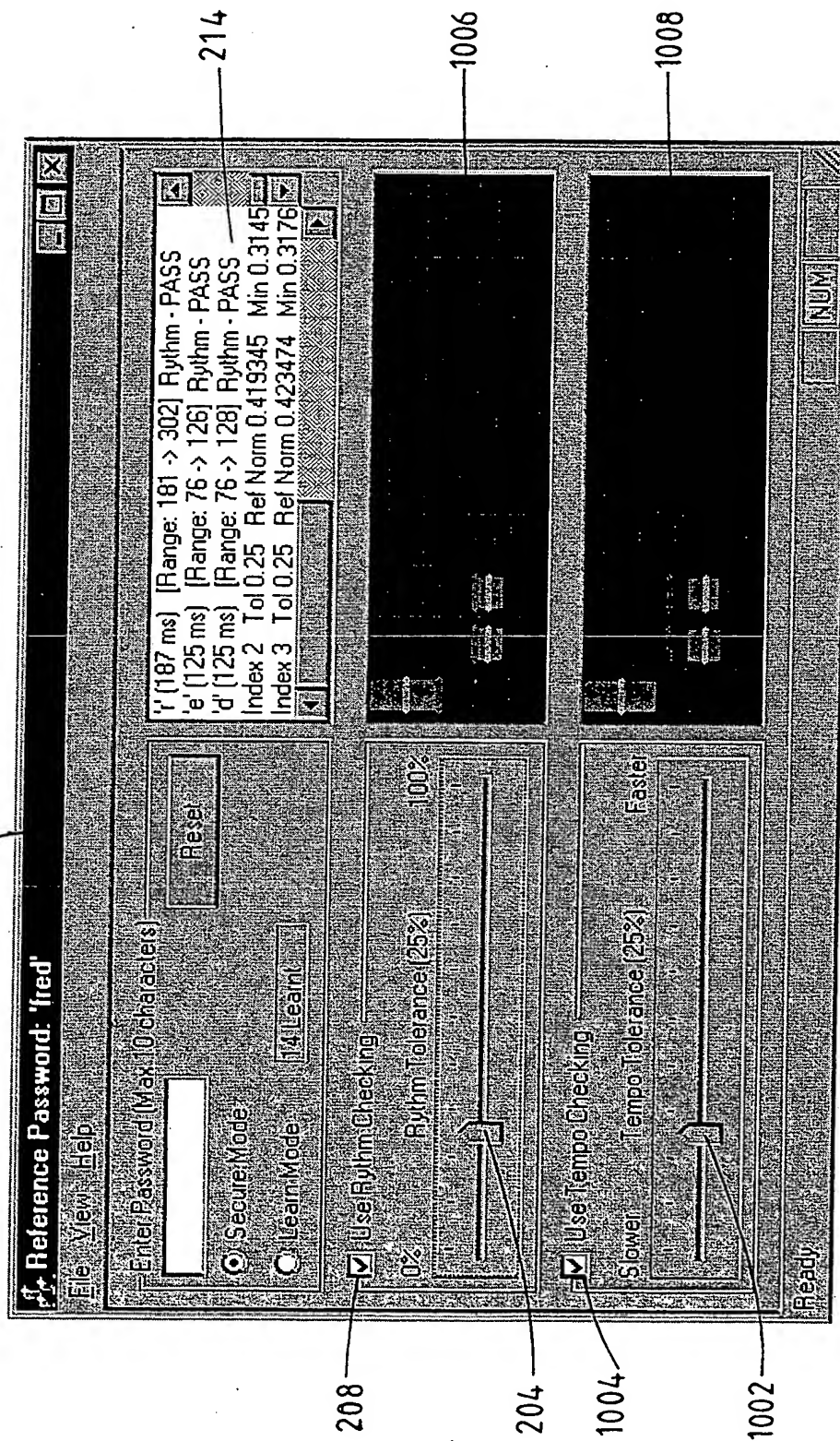
900FIG. 9

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

1000

202

FIG. 10

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)